PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-127969

(43)Date of publication of application : 25.05.1993

(51)Int.Cl. G06F 12/00
G06F 12/14

(21)Application number : 03-289757

(22)Date of filing : 06.11.1991

(71)Applicant : HITACHI LTD
HITACHI SEIBU SOFTWARE KK

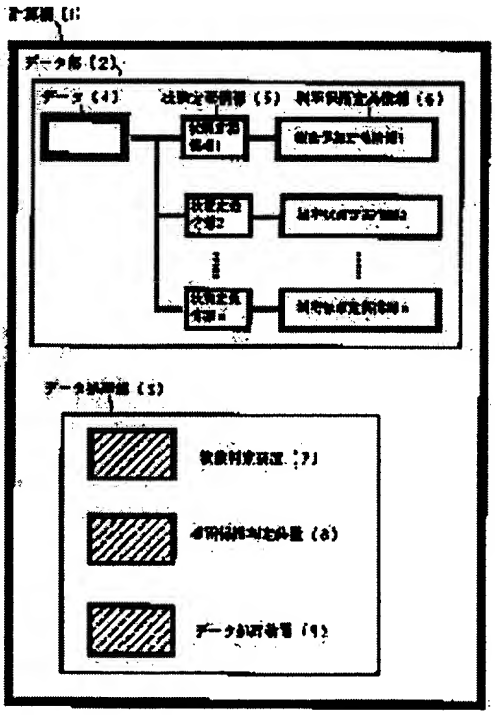
(72)Inventor : FUJIOKA NORIHIKO
TAKAHASHI NORIYUKI
NISHIMURA HIROKO
KUSHIRO YASUO

(54) SECRET INFORMATION PROTECTING METHOD

(57)Abstract:

PURPOSE: To execute different secret protection in accordance with the state of data by referring to the state definition information of the data stored before hand together with the data at the time of accessing to the data and discriminat ing the state of the data concerned.

CONSTITUTION: A computer 1 includes a data storage part 2 and a data processing part 3, and the data storage part 2 includes the data 4. The data processing part 3 is constituted to a state discriminating device 7, a secret protection discriminating device 8, and a data processor 9. Here, the data 4 taken out of the data storage part 2 is sent to the state discriminating device 7, and the state of the data 4 is discriminated. Besides, the data 4 is sent to the secret protection discriminating device 8, and the secret protection is executed in conformity with secret protection information in the state of the data 4, and at the time when access is to be suppressed, the transfer of the data 4 to the data processor 9 is suppressed. Besides, in the case that the access to the data 4 is permitted, the data 4 is sent to the data processor 9.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－127969

(43)公開日　平成５年(1993)５月25日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/00	５３７　Ａ	7832－5B		
	12/14	３２０　Ａ	9293－5B		

審査請求　未請求　請求項の数３(全 13 頁)

(21)出願番号　特願平3－289757

(22)出願日　平成３年(1991)11月６日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000233365
日立西部ソフトウエア株式会社
大阪府大阪市中央区北浜３丁目５番29号

(72)発明者　藤岡　典彦
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア開発本部内

(72)発明者　高橋　典幸
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア開発本部内

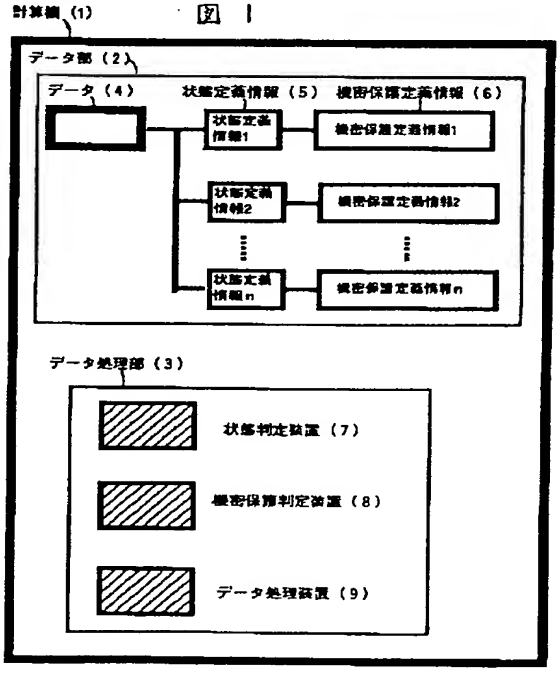
(74)代理人　弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　機密情報保護方法

(57)【要約】
【目的】データの状態の変化に従って異なる機密保護を施すことを可能にする。
【構成】計算機１はデータ４を含むデータ格納部２と状態判定装置７と機密保護判定装置８とデータ処理装置９を含むデータ処理部３を含む。
【効果】データの状態の変化に従って異なる機密保護を施すことが可能になる。

図１



1

【特許請求の範囲】

【請求項１】データの読みだしと更新及び削除を制限する機構を備えるデータ格納部及びデータ処理部を持つ計算機システムにおいて、状況に応じて変化するデータに対して、あらかじめ、データの状態の変化を定義する状態定義情報を一緒に格納しておき、該データから該状態定義情報を取り出して参照し、該状態定義情報からデータの状態の遷移を判定し、該状態に対応する固有の機密保護情報を割り当てることを特徴とする機密情報保護方法。

【請求項２】請求項１記載の機密情報保護方法においてあらかじめ、複数のデータを包含する集合データの状態の変化を定義する状態定義情報を一緒に格納しておき、該集合データから状態定義情報をとりだして参照し、該状態定義情報から集合データの状態を判定し、該状態に対応する固有に機密保護情報を割り当てることを特徴とする機密情報保護方法。

【請求項３】　請求項１記載の機密情報保護方法において時刻を監視する手段を設け、該手段から得られる時系列情報と状態定義情報を照合し、データの状態の遷移を判定する手段を持つことを特徴とする機密情報保護方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】計算機システムにおいてデータの読みだしと更新、及び削除を制限する機密保護の方式に関する

【０００２】

【従来の技術】従来、データに対する機密保護を行う技術には例えば、特開昭６２－２４８０４８号公報　ファイルの機密保護方式で示されるように複数のユーザからアクセス可能な共用のデータに対して読みだしと更新、及び削除を制限する手段としてデータに固有の機密保護情報を対応づけておく。機密保護情報には、読みだしと更新、及び削除を許可する権限コードが格納されており、データにアクセスする際にユーザに割り当てた権限コードと照合して、その結果に従って処理を行うか否かを判定して不当なデータアクセスを抑止していた。

【０００３】

【課題を解決するための手段】本発明の目的はデータの読みだしと更新及び削除を制限する機構を備えるデータ格納部及びデータ処理部を持つ計算機システムにおいて、状況に応じて変化するデータに対して、あらかじめ、データの状態の変化を定義する状態定義情報を一緒に格納しておき、保護を行おうとするデータから状態定義情報をとりだして参照し、該状態定義情報からデータの状態を判定し、該状態に固有に対応する機密保護情報を割り当てることで達成することができる。

【０００４】

【作用】データにアクセスする際にあらかじめデータと共に格納されたデータの状態定義情報を参照して当該データの状態を判定する。認識したデータの状態に対応した機密保護情報を参照して機密保護のための情報を取得してデータに対する不当な操作を抑止する。

【０００５】さらに複数のデータを含む集合データにも単体のデータと同様の処理を実現する。さらに時刻の変化にともなってデータの状態を制御する機構を付加してデータの状態の遷移を自動的におこなう。

【０００６】

【実施例】本発明の実施例を図面を用いて詳細に説明する。

【０００７】図１に本発明の基本的な構成を示す。計算機１はデータ格納部２とデータ処理部３を含む。データ格納部２はデータ４を含む。データ処理部３は状態判定装置７と機密保護判定装置８とデータ処理装置９から構成される。処理１－１においてデータ格納部２から取り出されたデータ４は状態判定装置７に送られる。状態判定装置７ではデータの状態を判定する。処理１－２においてデータは機密保護判定装置８に送られる。機密保護判定装置８おいてデータの当該状態における機密保護情報に従って機密保護を行い、アクセスを抑止するべき時には処理１－４においてデータをデータ処理装置９へ送ることを抑止する。また当該データへのアクセスを許可する場合においては処理１－４によりデータをデータ処理装置９へ送る。

【０００８】図２はデータ４の構成を示す。データ４はデータ本体部４－１と状態定義情報５と機密保護定義情報６から構成される。

【０００９】状態定義情報５は当該データが取りえる状態の数の定義があり、機密保護定義情報６は、状態定義情報５に対応づけられている。

【００１０】図３はデータ４の詳細を示す。データ４はデータ本体４－１と状態指示子４－２と状態定義情報５へのポインタを含む。状態指示子４－２はデータの状態を示すものでありデータの状態の変化にともなってその値を変化させる。状態定義情報５は、データがとることができる状態を示す状態定義値５－１と他の状態定義情報５へのポインタ５－２と当該状態時に対応する機密保護定義情報６へのポインタ５－３を含む。機密保護定義情報６はデータ本体４－１に対する読みだしと更新および削除の操作の許可または禁止の情報を含む。

【００１１】データ４をデータ処理部３で処理を行うとき状態判定装置７において状態指示子４－２を参照して、当該状態の状態定義情報５を選択してさらに当該状態に対応する機密保護定義情報６を選択する。次に機密保護判定装置において選択した機密保護定義情報６に基づいてデータ本体４－１に対する読みだしと更新及び削除の権限のチェックを行い、その結果それぞれの操作が許可されているときにはデータ処理装置９においてデータ本体４－１の操作を行う。

【００１２】図４はデータ処理部３の処理の流れを示す。

【００１３】データ４に対して読みだし・更新・削除の処理を行うとき、まず状態判定装置７でポインタ４－３をたどって状態定義情報５を選択する（処理１１１）。

【００１４】次に状態指示子４－２と状態定義値５－１を比較して（処理１１２）２つの値が一致すれば処理１１４へ処理を進める。２つの値が異なればポインタ５－２をたどって、次の状態定義情報５を選択して（処理１１３）さらに処理１１２を繰り返す。次に機密保護判定装置８でポインタ５－３をたどって当該状態時に対応する機密保護定義情報６を選択する（処理１１４）。

【００１５】次に当該処理が許可されているか否かを判定して（処理１１５）、当該処理が禁止されていれば操作不可のエラー処理を行い（処理１１７）、当該処理が許可されている場合にはデータ処理装置９においてデータ処理を実行する（処理１１８）。

【００１６】図５は図３に複数のデータ４を包含する集合データを定義する集合データ定義情報１２を追加したものである。集合データ定義情報１２には、集合データ名称１２－１と状態指示子１２－２とポインタ１２－３と集合データが含むデータ４を示すポインタ１２－４を含む。集合データ定義情報１２に対しても機密保護情報を割り当てて、単体のデータと同様の処理により集合データの機密保護を行うことができる。

【００１７】図６は、図１の構成に時刻監視装置１１を追加した構成図である。

【００１８】状態判定装置７において状態を判定する時に、時刻による状態定義情報と時刻を照合して当該時刻におけるデータの状態を判定することが出来る。

【００１９】図７は、図３のデータ部に状態制御情報を追加したデータ構造を示す。

【００２０】状態制御情報１０には状態変更時刻１０－１とポインタ１０－２を含む。状態変更時刻１０－２は、当該データ４が状態を遷移する時刻を格納しておき、ポインタ１０－２から遷移する状態の定義を示す。状態制御情報１０はデータ４の中のポインタ４－４から示される。

【００２１】図８に図４の処理に時刻による状態の制御を行う処理を示す。

【００２２】状態判定装置７でデータ４の状態を判定する前に処理２１１においてポインタ４－４をたどって状態制御情報１０を選択して処理２１２において状態変更時刻１０－１と現在の時刻を比較する。現在の時刻が状態変更時刻１０－１と等しいか過ぎているとき状態指示子４－２を更新する（処理２１３）。

【００２３】図９は、図１の構成において、状態判定装置７と機密保護判定装置８をデータ格納部２に移した構成である。データの機密保護をデータ格納部で行うことによりデータ処理部の処理負荷を軽減できる。

【００２４】図１０、図１１は本発明の具体的な実施例を示す図である。

【００２５】図１１は資料の置かれる変化に対応するその変化固有の機密保護マトリックスを示す。

【００２６】例えば、作成者Ａにおける資料の作成中という状態には図１１の①が対応し、読み書きが可能であるが、審査する人Ｂの資料の作成中という状態の場合には図１１の④が対応するため、読み書きはできない。

【００２７】また、資料の保存という状態では総合管理者Ｅに対して図１１の②が対応するため、総合管理者Ｅだけが資料を読むことのみが可能となり、他のＡ～Ｄには図１１の④が対応するため、その資料には読むことも書くこともできない。

【００２８】この図で示されるように資料の置かれる状態（データの変化）と権限を持つ人毎に対応する機密マトリックスが決まっているため、状態にあわせた機密保護が可能になる。

【００２９】

【発明の効果】本発明によりデータ状態遷移に従った機密保護を行える。また、単体のデータだけでなく、集合データについてもデータの状態遷移に応じた機密保護を行うことができる。さらに時刻の変化に基づくデータの状態遷移に応じた機密保護を行うことができる。

【図面の簡単な説明】

【図１】本発明の基本的な構成を示す図、

【図２】状態定義情報と機密保護定義情報を示す図、

【図３】状態定義情報と機密保護定義情報の詳細を示す図、

【図４】データ処理部の処理の流れを示すフローチャート、

【図５】集合データ情報を示す図、

【図６】本発明の構成に時刻監視装置を追加した構成を示す図、

【図７】データ部に状態制御情報を追加したデータ構造を示す図、

【図８】時刻による状態の制御を行う処理の流れを示すフローチャート、

【図９】状態判定装置と機密保護判定装置をデータ格納部に移した構成を示す図、

【図１０】本発明による具体的な実施例を示す図、

【図１１】機密保護マトリックスを示す図。

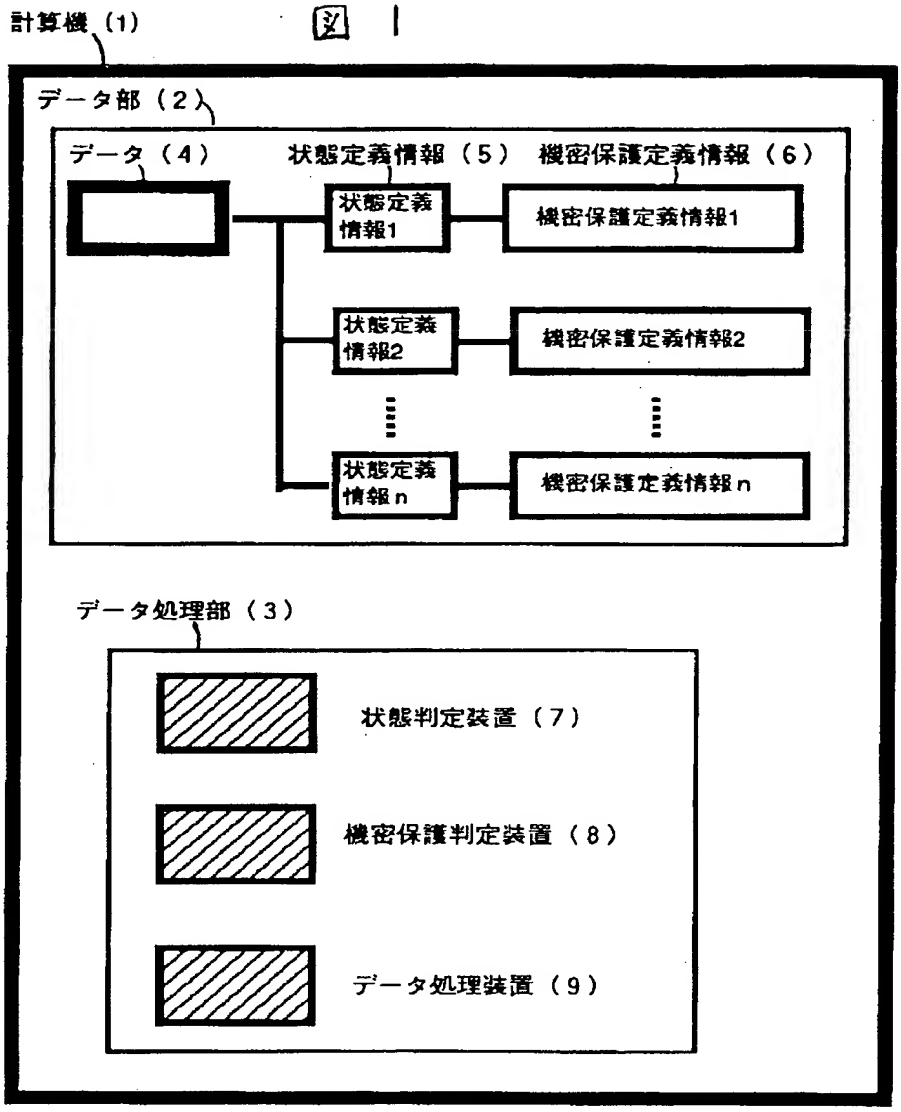
【符号の説明】

１…計算機
２…データ格納部
３…データ処理部
４…データ
５…状態定義情報
６…機密保護定義情報
７…状態判定装置
８…機密保護判定装置

5　　6

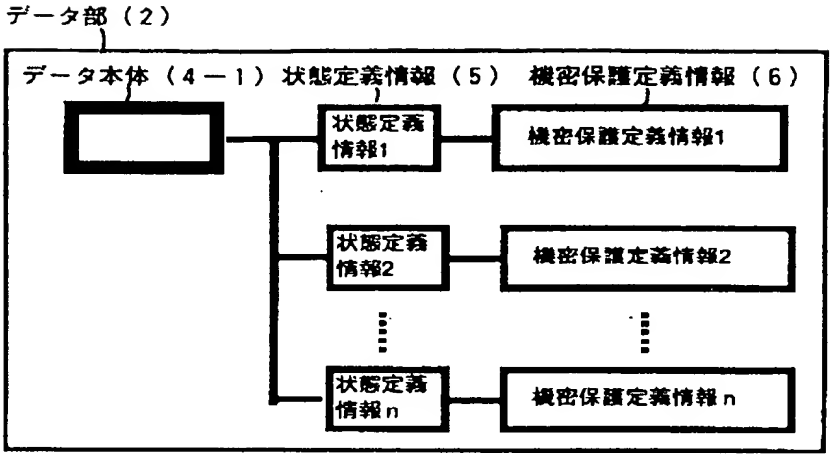
９…データ処理装置
１０…状態制御情報
＊１１…時刻監視装置
＊　１２…集合データ定義情報

【図１】



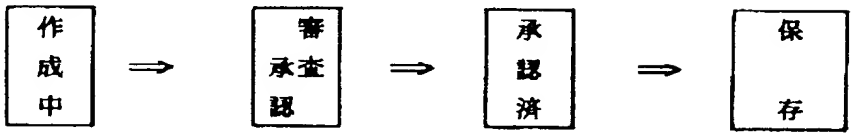
【図２】

図　２



【図１０】

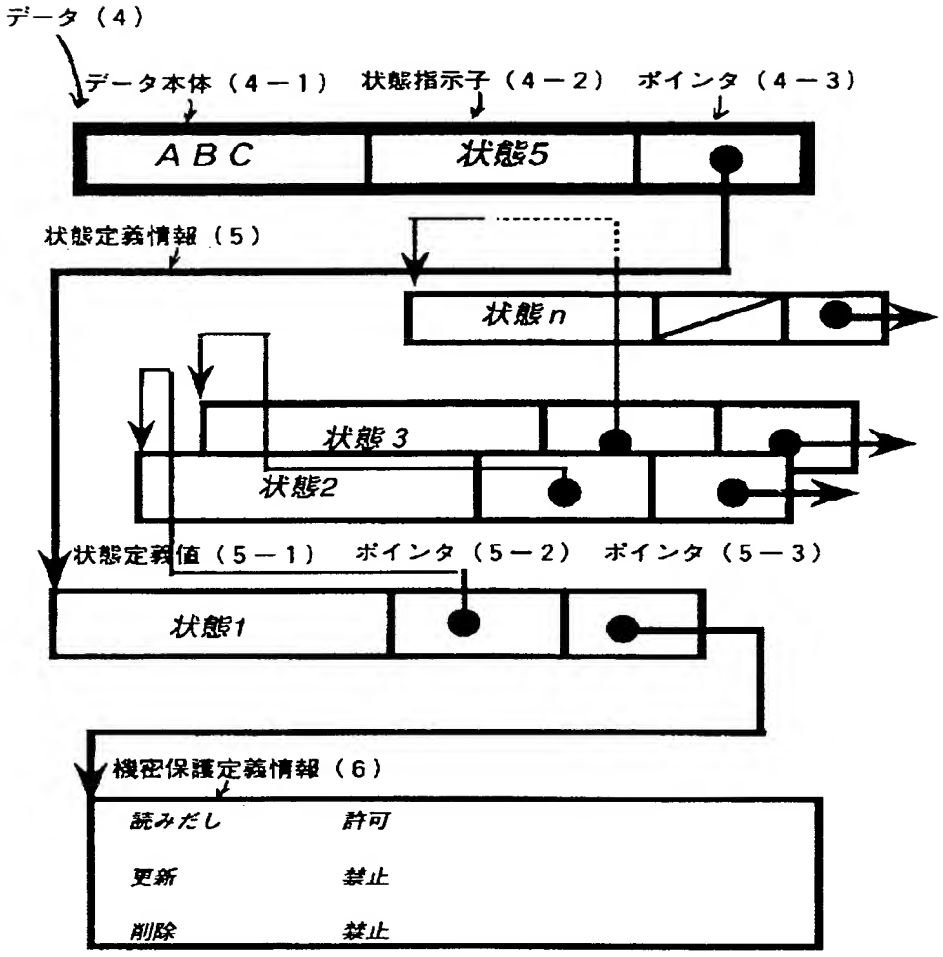
図１０



	READ	WRITE	READ	WRITE	READ	WRITE	READ	WRITE
作成者Ａ	○	○	○	×	○	×	×	×
一般の人Ｂ	×	×	×	×	○	×	×	×
審査する人Ｃ	×	×	○	○	○	×	×	×
承認する人Ｄ	×	×	○	○	○	×	×	×
総合管理者Ｅ	○	×	○	×	○	×	○	×

【図３】

図　３


データ（４）
データ本体（４－１）
状態指示子（４－２）
ポインタ（４－３）
ＡＢＣ
状態5
状態定義情報（５）
状態ｎ
状態３
状態2
状態定義値（５－１）
ポインタ（５－２）
ポインタ（５－３）
状態1
機密保護定義情報（６）
読みだし
許可
更新
禁止
削除
禁止

【図４】

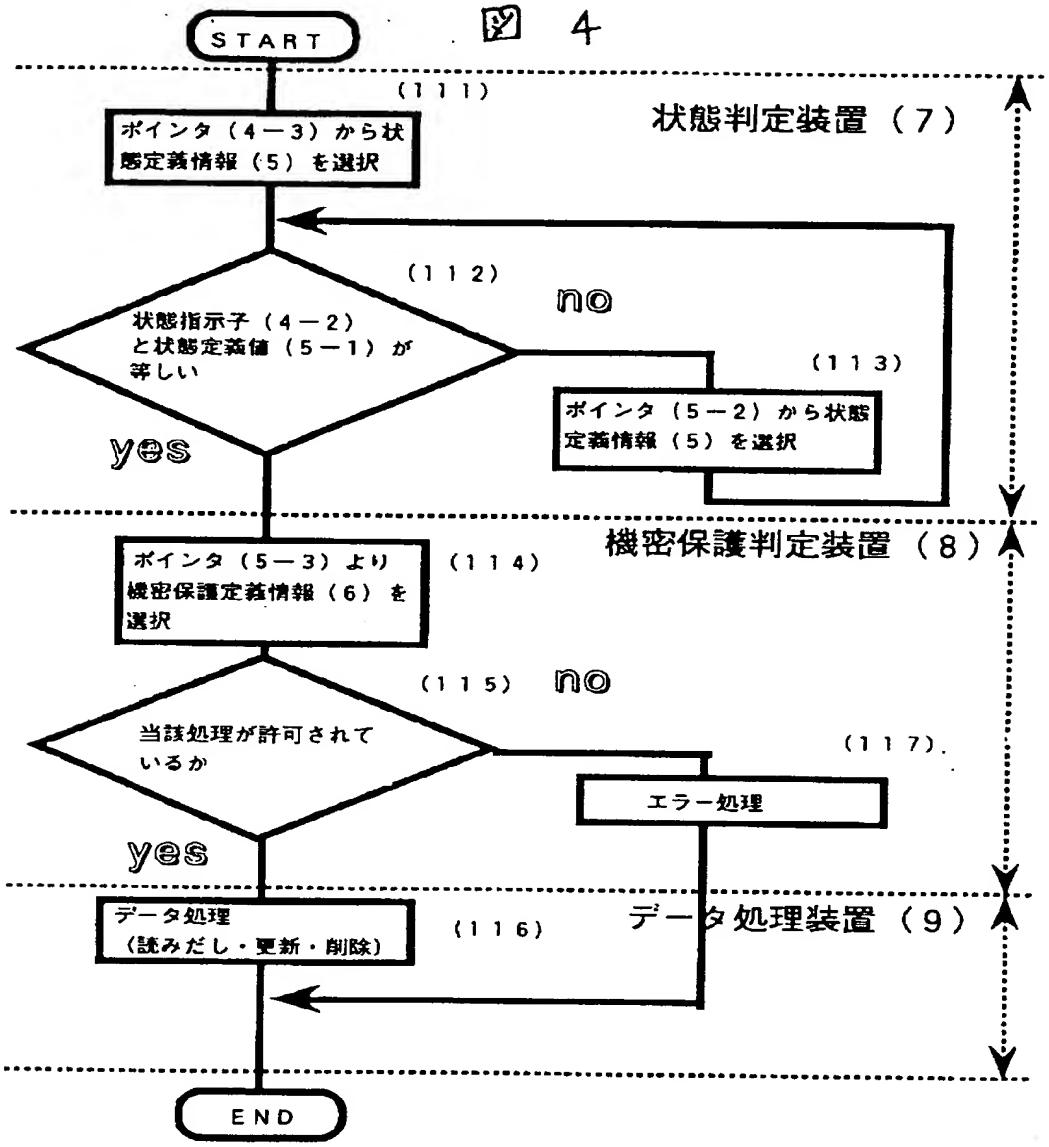
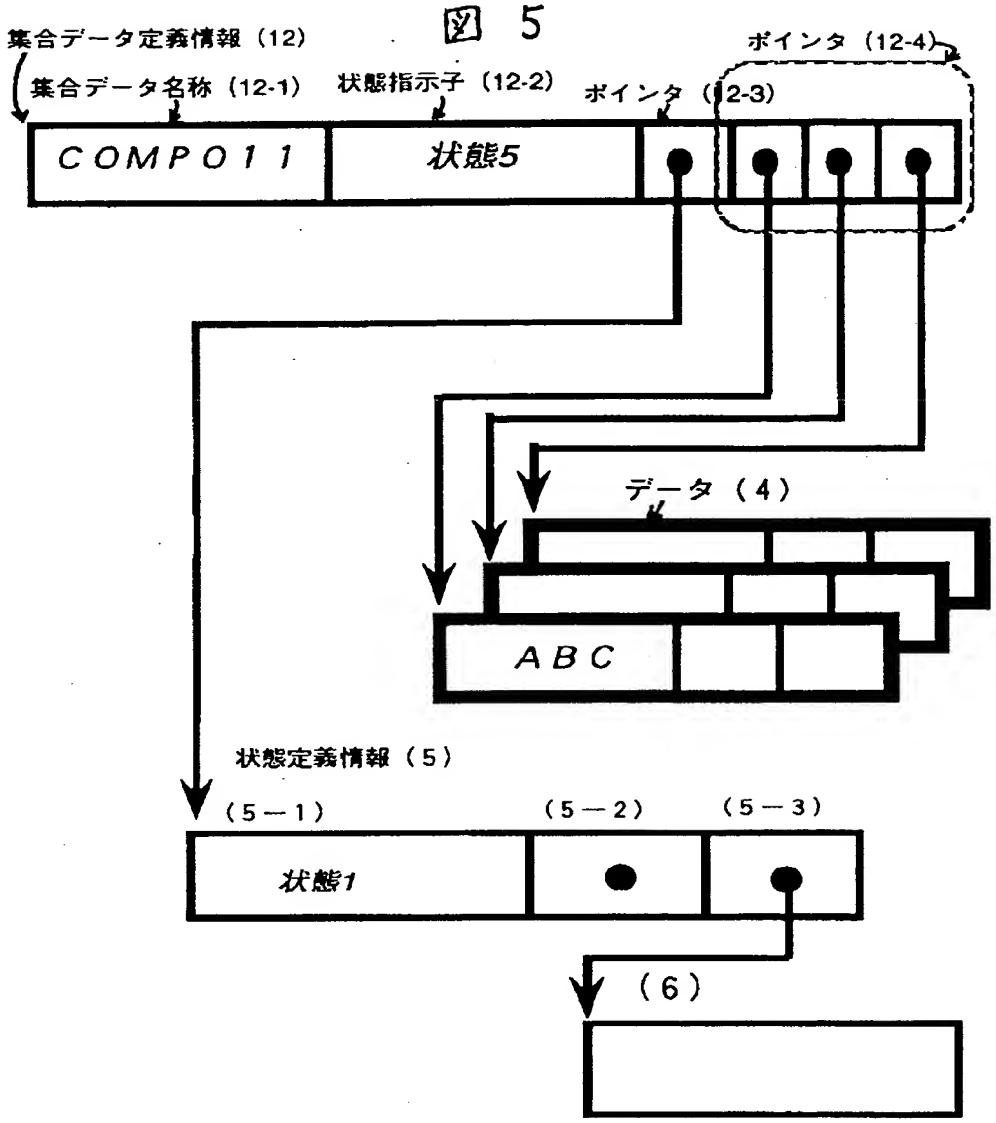


図 4
START
(111)
ポインタ（4－3）から状態定義情報（5）を選択
状態判定装置（7）
(112)
状態指示子（4－2）と状態定義値（5－1）が等しい
no
(113)
ポインタ（5－2）から状態定義情報（5）を選択
yes
機密保護判定装置（8）
ポインタ（5－3）より機密保護定義情報（6）を選択
(114)
(115)
no
当該処理が許可されているか
(117)
エラー処理
yes
データ処理（読みだし・更新・削除）
(116)
データ処理装置（9）
END

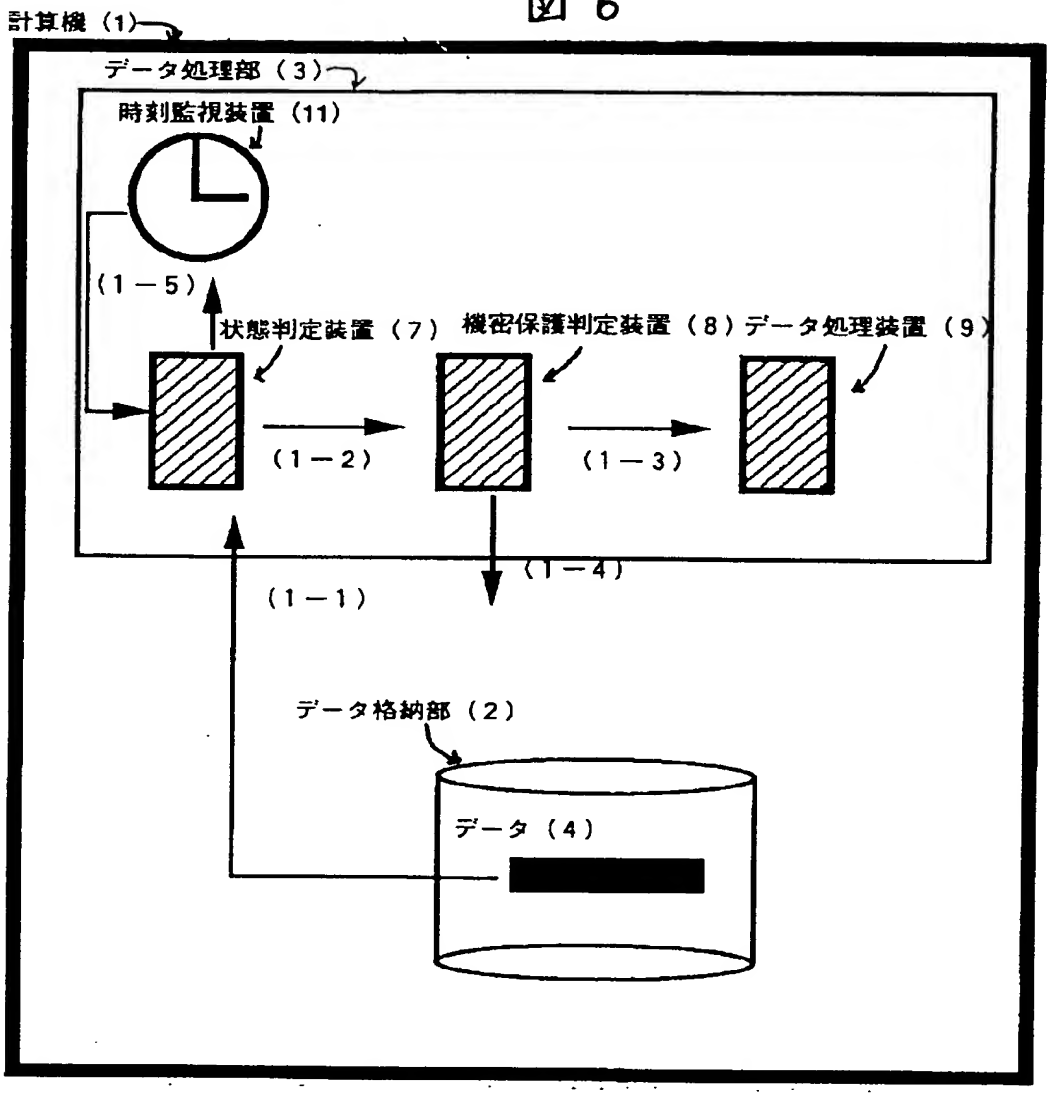
【図５】

図 5


集合データ定義情報（12）
集合データ名称（12-1）
状態指示子（12-2）
ポインタ（12-3）
ポインタ（12-4）
COMPO11
状態5
データ（4）
ABC
状態定義情報（5）
（5－1）
（5－2）
（5－3）
状態1
（6）

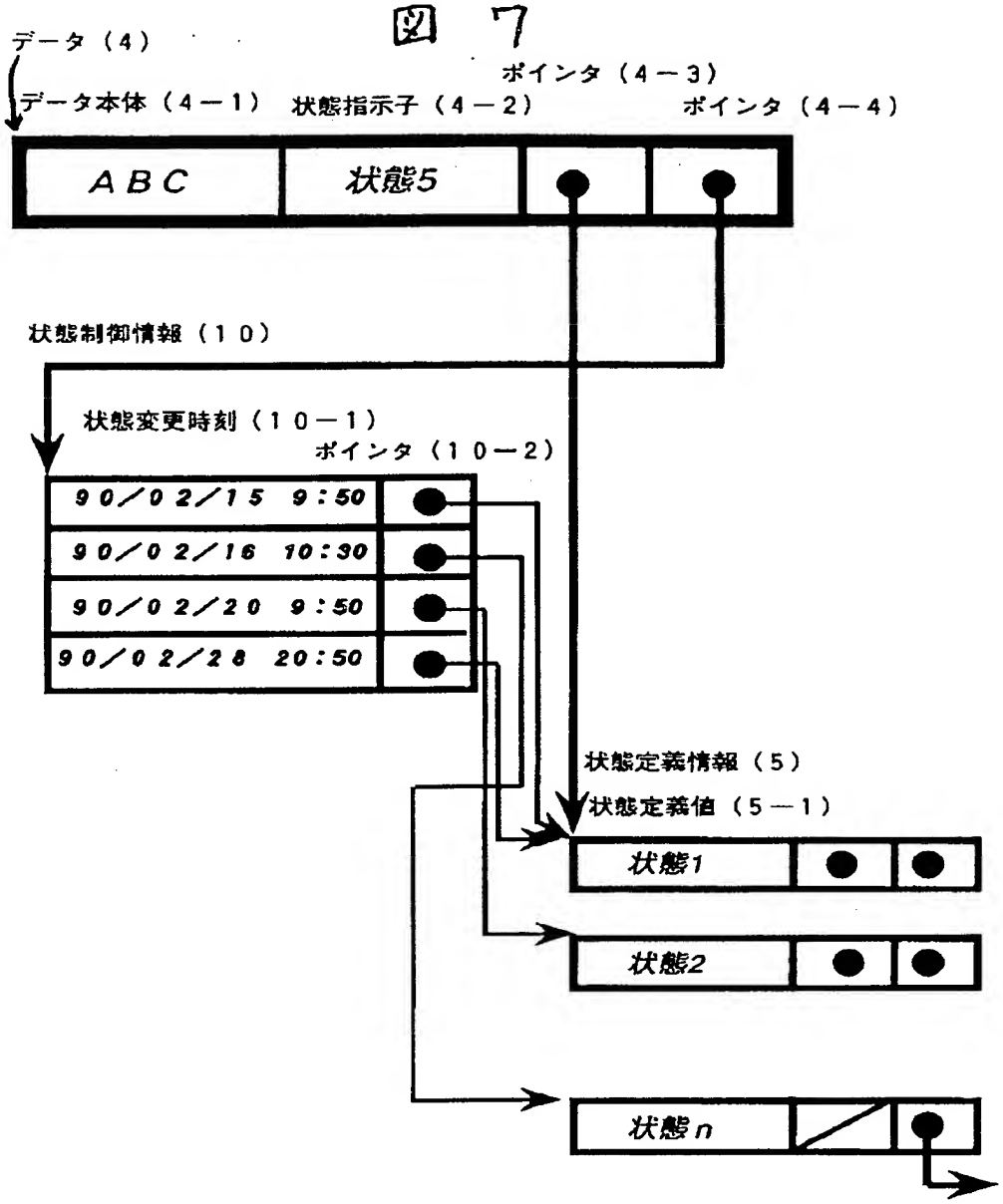
【図６】

図 6


計算機（1）
データ処理部（３）
時刻監視装置（11）
（1－5）
状態判定装置（７）
機密保護判定装置（８）
データ処理装置（９）
（1－2）
（1－3）
（1－4）
（1－1）
データ格納部（２）
データ（４）

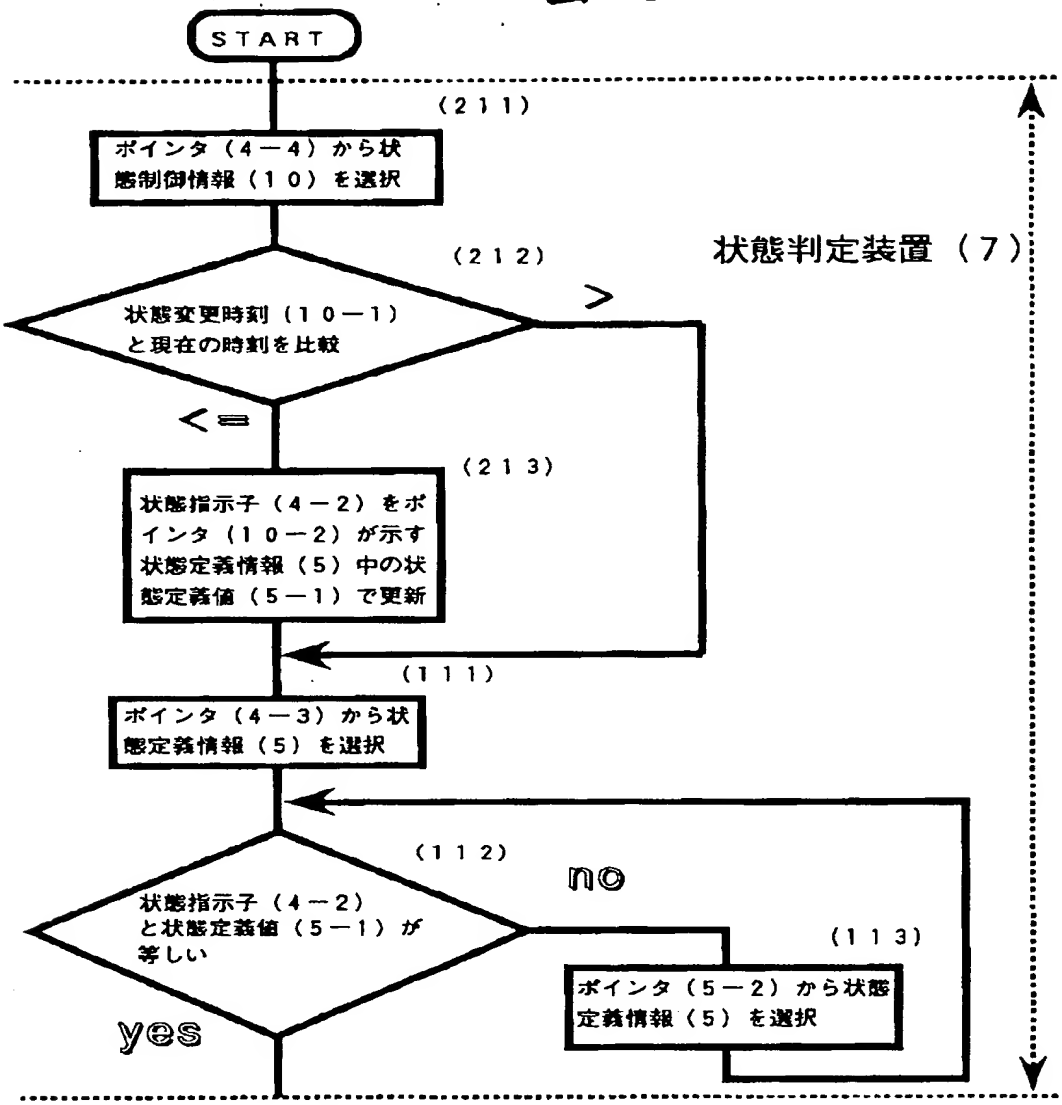
【図７】

図　７


データ（４）
データ本体（４－１）
状態指示子（４－２）
ポインタ（４－３）
ポインタ（４－４）
ＡＢＣ
状態5
状態制御情報（１０）
状態変更時刻（１０－１）
ポインタ（１０－２）
９０／０２／１５　９：５０
９０／０２／１６　１０：３０
９０／０２／２０　９：５０
９０／０２／２８　２０：５０
状態定義情報（５）
状態定義値（５－１）
状態1
状態2
状態ｎ

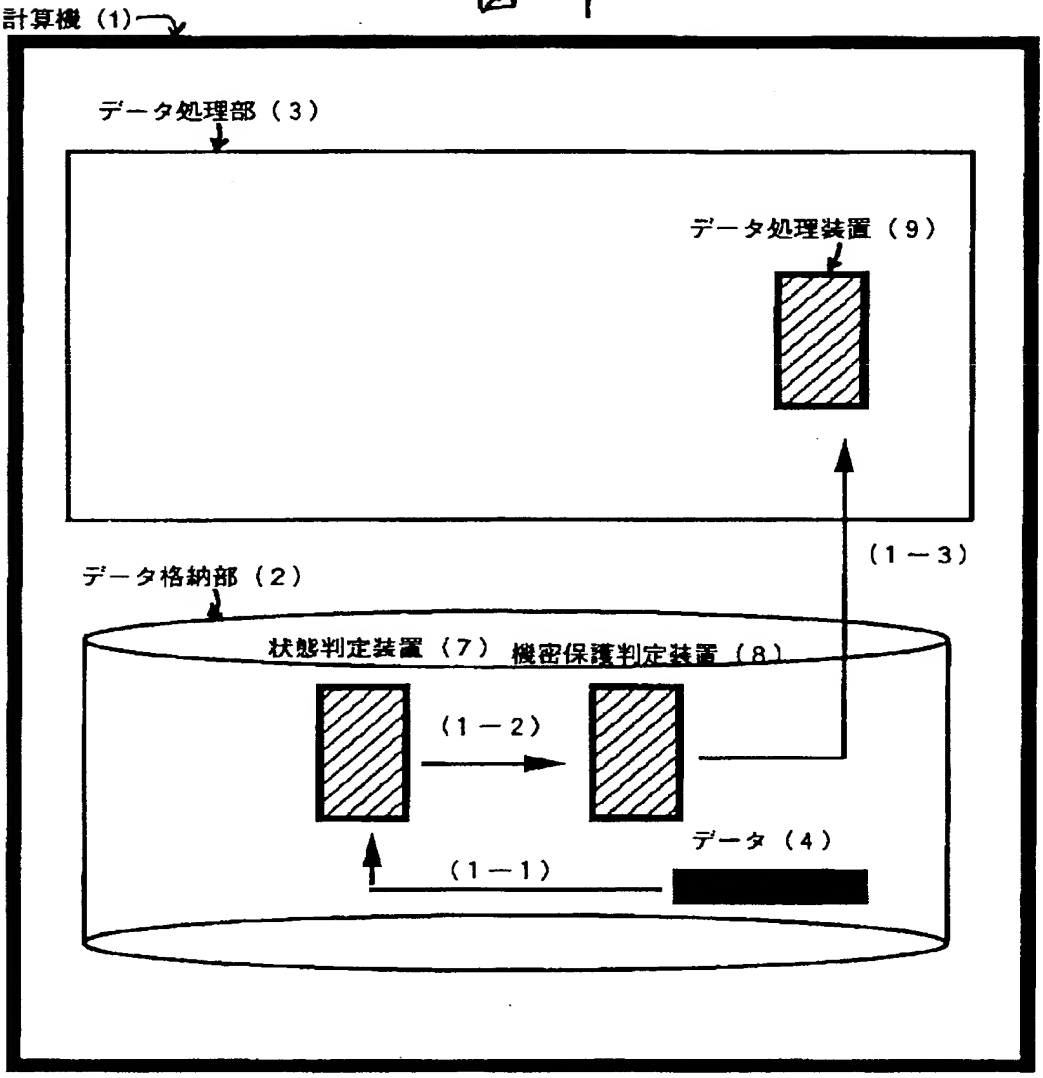
【図８】

図　８


START
(211)
ポインタ（４－４）から状態制御情報（１０）を選択
(212)
状態変更時刻（１０－１）と現在の時刻を比較
>
<=
(213)
状態指示子（４－２）をポインタ（１０－２）が示す状態定義情報（５）中の状態定義値（５－１）で更新
(111)
ポインタ（４－３）から状態定義情報（５）を選択
(112)
状態指示子（４－２）と状態定義値（５－１）が等しい
no
(113)
ポインタ（５－２）から状態定義情報（５）を選択
yes
状態判定装置（７）

【図９】

図 9


計算機（1）
データ処理部（３）
データ処理装置（９）
（１－３）
データ格納部（２）
状態判定装置（７）
機密保護判定装置（８）
（１－２）
データ（４）
（１－１）

【図１１】

図１１

機密保護マトリックス

	READ	WRITE
①	○	○
②	○	×
③	×	○
④	×	×

フロントページの続き

(72)発明者　西村　弘子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウエア開発本部内

(72)発明者　久代　康雄
大阪府大阪市中央区北浜三丁目５番29号　日立西部ソフトウエア株式会社内

THIS PAGE BLANK (USPTO)